UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,971	04/06/2001	Olli Immonen	061602-1525	8278

30542 7590 05/15/2007
FOLEY & LARDNER LLP
P.O. BOX 80278
SAN DIEGO, CA 92138-0278

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/720,971	**Applicant(s)** IMMONEN, OLLI	
	Examiner Zachary A. Davis	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,15-40 and 42-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,15-40 and 42-68* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. A response was received on 07 March 2007. By this response, Claims 8 and 24 have been amended. No claims have been added or canceled. Claims 1-12, 15-40, and 42-68 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 07 March 2007 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1, 3-12, 15-19, 21-24, 27-40, 42-44, and 46-68 under 35 U.S.C. 103(a) as unpatentable over Ichikawa, PCT Publication WO97/24831, in view of Anvret et al, European Publication EP 0538216, and Fang et al, US Patent 6240512, and in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Specifically, in arguments solely directed to the Ichikawa reference, Applicant first argues that Ichikawa is not directed to wireless telecommunications apparatus or wireless application protocols (pages 17-18 of the present response). However, the Examiner disagrees, noting that, as cited by Applicant, Ichikawa discloses the use of smartcards in wireless telecommunications apparatus (page 2, lines 3-25); the Examiner further notes that the disclosure of a smartcard implemented with an ATM is cited only as an example and not as a limiting embodiment (see Ichikawa, lines 14-17, where the ATM is used as an example of the general operation; see also page 14, lines 4-9). Additionally, although Ichikawa does not explicitly disclose the specific "wireless application protocol", the Examiner notes that the claimed term "wireless application protocol" is not given any patentable weight, because the term appears only in the preamble of the claims and does not further limit any structure or step recited within the body of the claims.

Applicant further argues that Ichikawa does not disclose sending information regarding the selection algorithm itself (page 19 of the present response) and that Ichikawa does not describe sending any information regarding at least one algorithm (page 18). However, the Examiner notes that it was not stated that the selection algorithm in Ichikawa (page 11, lines 1-8, as cited by Applicant, for example) corresponded to the claimed algorithm; rather, the Examiner's interpretation is that the selected series number is what actually provides the information regarding the selected algorithm (i.e. the variation of the series number is equivalent to variation of the algorithm used in generating).

The Examiner notes that Applicant argues that the claimed master secret code has been mapped to both the "derived key" and the "master key" as disclosed in Ichikawa (see page 20 of the present response, where Applicant alleges that the Examiner's interpretation was of the derived key reading on the claimed master secret code, and page 24, where Applicant implies that the master key in Ichikawa corresponds to the claimed master secret code). This contradiction makes it unclear which interpretation Applicant has taken. To clarify, the Examiner intended that the "master key" in Ichikawa corresponded to the claimed master secret code, as the Examiner believed was the clear interpretation of the cited portions of Ichikawa (notably page 4, lines 5-15, for example).

Applicant further argues that the derived key may or may not be used to generate the electronic signature in Ichikawa, based on the assumption that the derived key was interpreted as reading on the claimed master secret code (see page 20 of the present response). However, as noted above, the derived key was not interpreted as reading on the master secret code, but instead it was the master key, and thus the arguments based on this alternate interpretation are not given any weight. The Examiner again notes that, specifically in response to the arguments regarding the disclosure of the signature in Ichikawa (page 20 of the present response), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. Specifically, deficiencies in Ichikawa's disclosure of the generation of the signature are remedied by the other references as set forth below.

Turning to the Anvret reference, Applicant further argues that Anvret only shows storage of public RSA keys, but does not show storage or use of a private key (page 21 of the present response). The Examiner respectfully disagrees. As previously noted, Anvret discloses the use storage of variables "a" and "q" which are used in deriving a key, i.e. as a master secret code for deriving a signature as claimed (column 5, lines 53-

58). The Examiner further notes that Anvret explicitly discloses not only use and storage of an RSA public key but also use and storage of a private key (see column 5, lines 23-44, where “open”, i.e. public, and “secret”, i.e. private, keys are assigned, and lines 45-50, where the keys and encryption/decryption transformations are stored in the smart card). Further in response to the argument that the key in Anvret is not associated with an algorithm; however, the Examiner respectfully disagrees, noting in particular the disclosure of column 6, line 28-column 7, line 13, where a particular process or algorithm for generating the signature is disclosed. The Examiner additionally notes the discussion of the use of the RSA algorithm (see column 5, lines 23-59).

Further, in response to applicant's argument that Fang is nonanalogous art (page 22 of the present response), it has been held that a prior art reference must either be in the field of applicant’s endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Fang is generally related to the same field of the applicant’s endeavor, noting that Applicant discloses that the claimed invention is directed to establishing a secure connection (see page 4, paragraph 0005 of the substitute specification received 15 August 2005) and that Fang is also generally related to establishment of secure connections, particular in regards to single sign-on processes used for authentication (see Fang, column 2, lines 25-31, for example).

Applicant argues that Fang does not teach generating a master key in response to a message (page 22 of the present response). However, the Examiner does believe that the cited portion of Fang does, in fact, disclose generating a master key in response to a message; namely, it is clear that because the master keys are distributed in response to the administrator's initiation, then this initiation must include some sort of message indicating distribution of the keys is to take place (Fang, column 9, lines 9-15).

Applicant further alleges that the Examiner previously admitted that "any key or other variable that can be changed at will is not a master key or code" (page 23 of the present response). The Examiner respectfully submits that this is a misapprehension of the Examiner's statement in the previous Office action that the cited portion of Anvret, namely column 7, lines 12-13, stating that X is changed for each session would itself imply that X is not, in fact, a master key or code. The Examiner notes that if a key X is changed for each session, then by definition, X is a session key. It should further have been clear from the surrounding context (see column 6, line 28-column 7, line 13) that X is clearly derived from other keys and variables, and would generally not have been considered a master key. The alleged broad admission noted above does not follow from the specific statement made by the Examiner. Specifically, it does not logically follow that Anvret states that a master key can never change, nor has the Examiner made such an allegation.

In response to applicant's argument that because the derived key of Ichikawa (alleged to correspond to the claimed master secret code; this assertion was addressed above) is generated in both the client and server of Ichikawa, but the master key in

Fang is allegedly only generated at one server (to be addressed below), then the combination would be inoperable (page 23 of the present response), the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In particular, in response to the allegation that the master key in Fang is only generated at one server (page 23 of the present response) and then distributed, the Examiner respectfully disagrees, noting that the cited portion of Fang does not disclose "distribution" but rather "resynchronization" of the keys (column 9, lines 9-15), which suggests that each entity generates its own new version of the keys. Further in response to the allegation that the server in Fang is not analogous to a data communication apparatus, the Examiner respectfully disagrees, noting that a server by definition is a type of data communication apparatus.

Regarding the rejection of Claims 2, 20, 25, 26, and 45 under 35 U.S.C. 103(a) as unpatentable over Ichikawa in view of Anvret and Fang and further in view of Weiss, US Patent 5845519, Applicant argues that Ichikawa teaches that the master key should be stored in permanent memory (page 24 of the present response, citing page 4, lines 5-8 of Ichikawa) and that one would not be motivated to modify the invention to have the master key stored for a predefined period of time. However, the Examiner notes that the combination of Ichikawa, Anvret, and Fang does, in fact, teach changing the master key (see, for example, Fang, column 9, lines 9-15, as previously cited). Further, the Examiner notes that the claimed "predefined period of time" does not necessarily preclude permanent storage.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Specification

3. The Examiner thanks Applicant for correcting the errors as noted in the previous Office action and other errors not specifically noted. However, the objection to the disclosure is not withdrawn, as the amendment to the specification has introduced new errors not previously present in the disclosure.

4. The disclosure is objected to because of the following informalities:

The specification contains minor grammatical errors. For example, in paragraph 0009 (as amended at page 2 of the present response), the phrase "the user pays less when re-establishing a secure session, in a case when necessary information for re-establishing is saved" is still generally unclear grammatically.

Appropriate correction is required. Applicant's cooperation is again requested in correcting any other errors of which applicant may become aware in the specification.

Claim Objections

5. The objection to Claim 24 is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3-12, 15-19, 21-24, 27-40, 42-44, and 46-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa, PCT Publication WO97/24831, in view of Anvret et al, European Publication EP 0538216, and Fang et al, US Patent 6240512.

In reference to Claim 1, Ichikawa discloses a method that includes connecting a wireless communication apparatus to a separate unit; accessing a wireless communication network (page 2, line 16-page 3, line 12); transmitting a request, which includes information on which of at least one algorithm the wireless apparatus supports, from the wireless apparatus to a data communication apparatus (page 10, line 14-page 11, line 11); the data communication apparatus choosing an algorithm and transmitting a message, which includes information about the chosen algorithm, to the wireless apparatus (page 9, lines 13-23); the wireless apparatus generating a master secret code (page 4, lines 10-12) and calculating a signature based on the chosen algorithm and the master secret code (page 4, lines 12-15); and saving the master secret code on a memory means of the separate unit and in the data communication apparatus (page 7, line 3-page 8, line 4). However, Ichikawa does not explicitly disclose the use of public and private keys.

Anvret discloses a method that includes the use of public and private keys in message communication (column 6, lines 1-11 and 47-48); transmitting a message, which includes the public key, to a wireless communication apparatus (column 6, lines 39-41); transmitting a response, which includes a calculated signature, to a data communication apparatus (column 6, lines 28-41); the data communication apparatus calculating a master secret code based on a chosen algorithm, a received signature, and the private key; and establishing a secure connection between the wireless apparatus and the data communication apparatus (column 6, line 28-column 7, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Ichikawa's method of generating encryption keys with Anvret's method of identification and exchange of encryption keys, in order to promote the usage of smart cards that enable strong algorithms and enhanced security (see Anvret, column 1, lines 23-25).

However, neither Ichikawa nor Anvret explicitly discloses an apparatus generating a master secret code specifically in response to a message. Fang discloses a method in which a master code is generated in response to a message (see column 9, lines 9-15, where master keys are resynchronized in response to initiation by an administrator). Therefore, it would have been obvious to modify the method of Ichikawa and Anvret by including generation of a master code in response to a message, in order to alleviate security concerns, particularly in regard to key exposure (see Fang, column 9, lines 9-11 and 51-53).

In reference to Claim 3, Ichikawa, Anvret, and Fang further disclose re-establishing a connection by transmitting a request, which includes a calculated signature based on the algorithm, public key, and stored secret, from the wireless apparatus to the data communication apparatus (Anvret, column 6, lines 1-11, 39-41, and 47-48). Ichikawa, Anvret, and Fang additionally disclose that the data communication apparatus calculates the master secret code based on the algorithm, signature, and private key, and establishes a secure connection to the wireless apparatus (Anvret, column 6, line 28-column 7, line 13).

In reference to Claim 4 and 27, Ichikawa, Anvret, and Fang further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

Claims 5, 15, 19, 22-24, and 46 each recite limitations recited in, and are substantially equivalent to, Claim 1. The claims are therefore rejected by a similar rationale.

In reference to Claim 6, Ichikawa, Anvret, and Fang further disclose a wireless communication apparatus having an exchangeable memory means (Ichikawa, namely the smart card of page 2, lines 16-25; Anvret, column 2, lines 37-41).

In reference to Claims 7-10, 28-35, 48, 49, and 52-55, Ichikawa, Anvret, and Fang further disclose that the master secret code and signature are each stored and generated on the separate unit (Ichikawa, Figure 1; page 4, lines 2-15).

In reference to Claims 11, 18, 21, 36-40, 43, 44, and 56-64, Ichikawa, Anvret, and Fang further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

In reference to Claims 12 and 65-68, Ichikawa, Anvret, and Fang further disclose that the separate unit is a subscriber identity module (Ichikawa, page 2, lines 16-25).

In reference to Claim 16, Ichikawa, Anvret, and Fang further disclose encryption means for encrypting the master secret (Ichikawa, page 11, line 19-page 12, line 2).

In reference to Claims 17 and 42, Ichikawa, Anvret, and Fang further disclose a secure database including at least one master code or signature (Ichikawa, page 4, lines 12-15; Figure 5; page 7, line 9-page 8, line 10; page 11, line 19-page 12, line 2).

Claim 47 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 50 and 51, Ichikawa, Anvret, and Fang further disclose a processor generating the master secret code (Ichikawa, page 4, lines 2-15).

8. Claims 2, 20, 25, 26, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Anvret and Fang as applied to claims 1 and 19 above, and further in view of Weiss, US Patent 5845519.

In reference to Claims 2 and 20, Ichikawa as modified discloses everything as applied to Claims 1 and 19 above. However, although Ichikawa, Anvret, and Fang disclose changing a master secret (see Fang, column 9, lines 9-11 and 51-53), none of Ichikawa, Anvret, or Fang explicitly discloses saving the master secret for a predefined time. Weiss discloses saving a master key for a predetermined time (column 12, lines 40-61). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of encryption key exchange taught by Ichikawa, Anvret, and Fang with Weiss' teaching of saving keys for a predefined time, in order to prevent an unauthorized user from compromising the key (see Weiss, column 12, lines 40-61).

Claim 25 corresponds substantially to Claim 3, and is rejected by a similar rationale.

In reference to Claims 26 and 45, Ichikawa, Anvret, Fang, and Weiss further disclose that the separate unit is a smart card (Ichikawa, page 2, lines 16-25; Anvret, column 5, lines 45-58, for example; Fang, column 8, lines 17-25).

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER